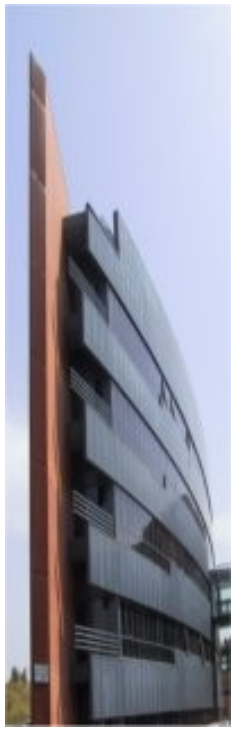
Donde Doy otro Susto en las redes académicas

Victor Barahona

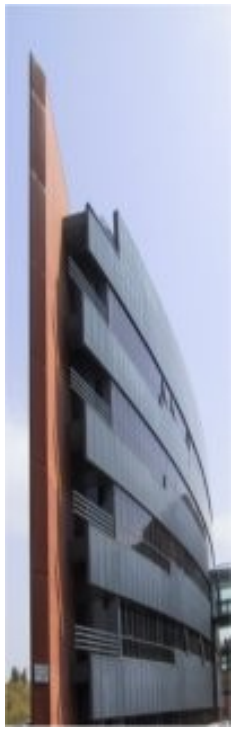
Universidad Autónoma de Madrid

GGTT Cordoba 2016



Los síntomas

- ¡La red no va!
- OSPF down
- Pocos e inconsistentes logs
- Ausencia de registros de netflow
- 6 veces en 2 años
- Normalmente en vacaciones



El Susto

- 6 Abril mie 19:46-21:10
- DDoS contra una IP
- Origen >65000 IPs
- SSH y Auth
- TCP-SYN
- 2.2Gb/s
- ¡2x380Kpps!

Summary

Severity Level:	Severity Percent:	Impact:	Direction:	Misuse Types:	Managed Object:	Target:
High	7,599.0% of 10 Kpps Top Misuse Type: **TCP SYN**	291.9 Mbps/760.1 Kpps at Network Boundary	Incoming	TCP SYN, TCP RST	UAM	150.244

Alert Traffic

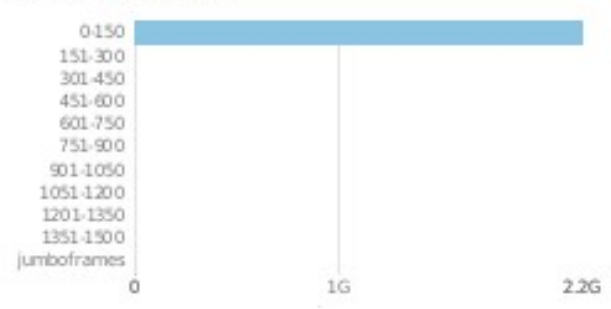
Top Traffic Patterns (last 5 minutes)

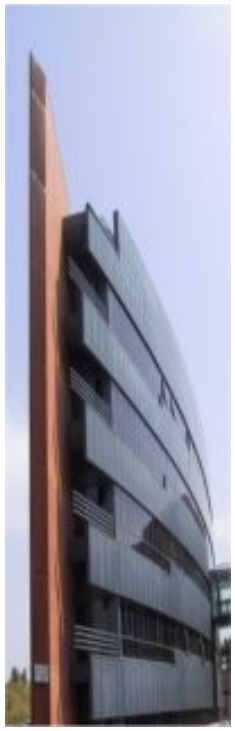
	Source	Protocol	Flags	Src Port	Destination	Dest Port	Router	Alert Traffic
1.	Highly Distributed	TCP	SR	1024 - 65535 (Dynamic)	150.244	113 (auth)	Telmad-RT4	185.50 Kpps

Alert Characterization

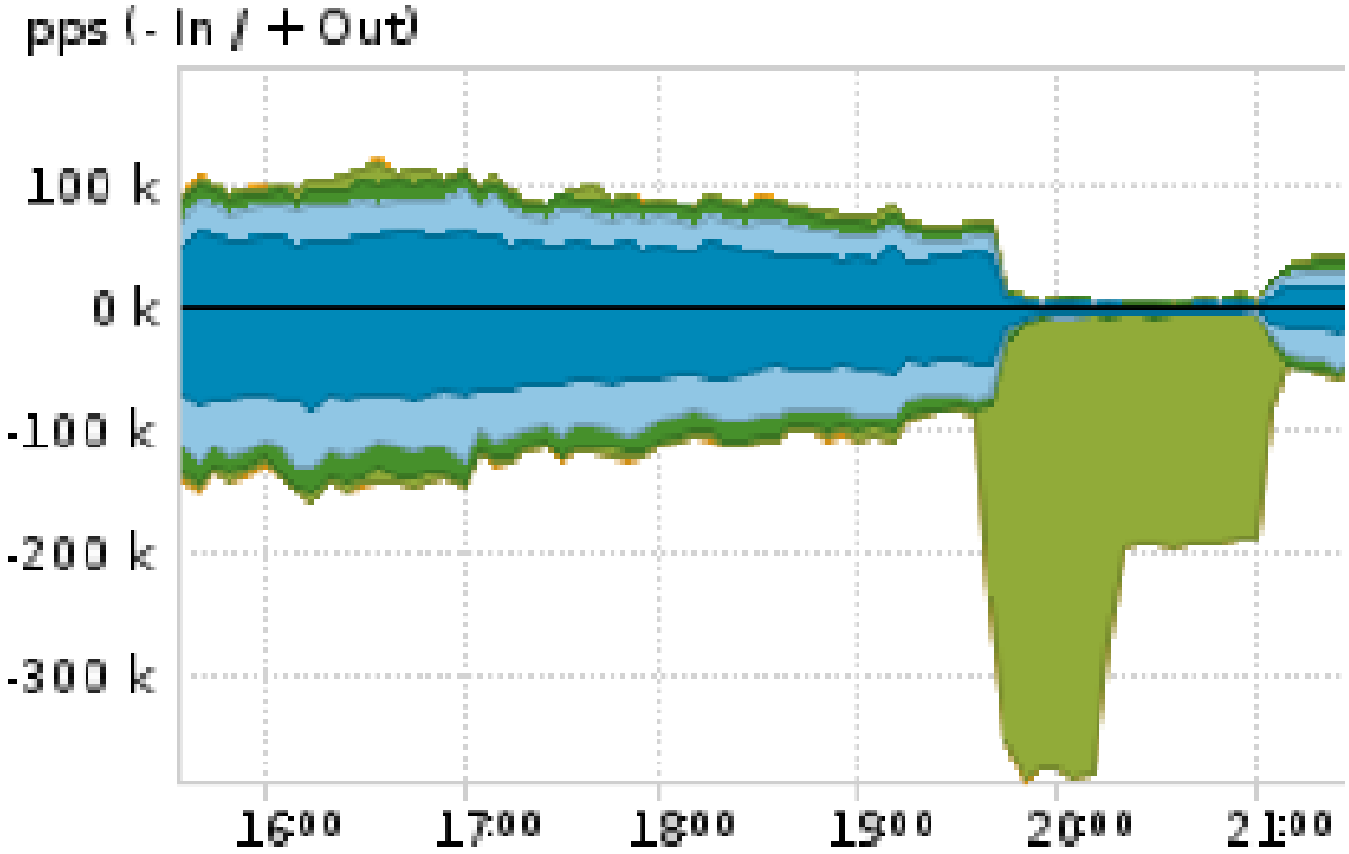
Protocols	tcp (6)	100.00%
Source IP Addresses	Highly Distributed	100.00%
Destination IP Addresses	150.244	100.00%
TCP Flags	S (Synchronize)	100.00%
Misuse Types	TCP SYN (5)	100.00%
Source TCP Ports	1024-65535 (Dynamic)	98.00%
Destination TCP Ports	113 (auth)	55.00%
Destination TCP Ports	22 (ssh)	44.00%

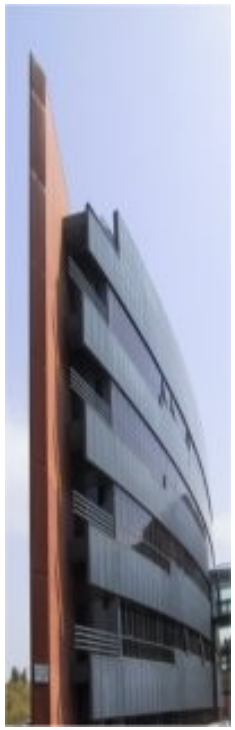
Packet Size Distribution





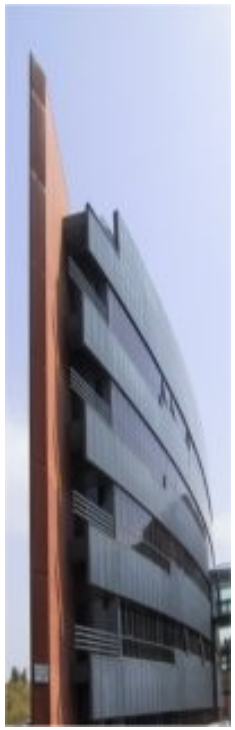
Ataque TCP-SYN DDoS





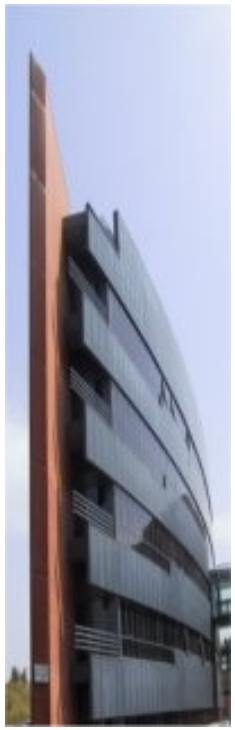
Datos DDoS Q1 2016

- Q1>23%
- 2015>111%
- Origen del 80%: CN, US, KR
- El 70% no supera las 4h
- El mas largo 8,9 dias
- UDP, SYN, TCP y HTTP
- Bigger DDoS 274 Gbps/27 Mpps



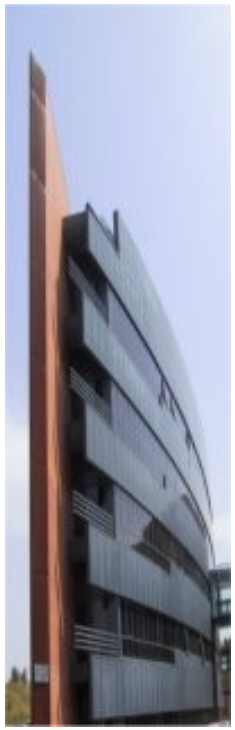
Riesgo

- Normalmente motivaciones económicas o políticas
- Las universidades no somos un objetivo prioritario. Pero...
- Cada vez es más asequible la infraestructura DDoS
- A menor costo mayor probabilidad



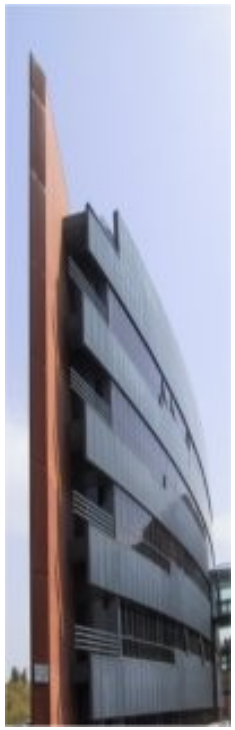
Medidas antes del ataque

- Muy básicas
- Solíamos ser origen de los ataques
- Límite de 3000 conexiones simultaneas por equipo propio.



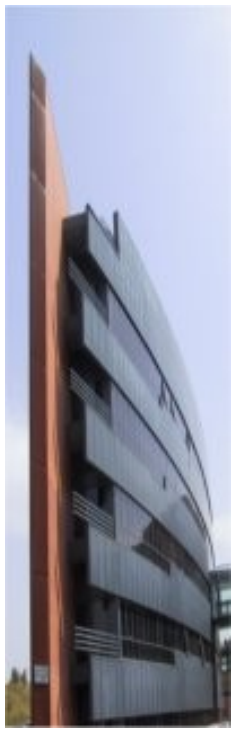
Medidas después del ataque

- Límite en el número global de conexiones desde la zona Internet
- Límite en el número de conexiones por IP origen desde la zona Internet
- Acceso de backup
- Mejoras en el sistema de análisis de flujos.



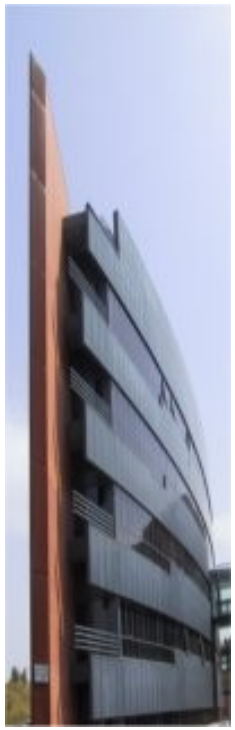
Medidas exteras a explorar

- Servicios de contención DDoS en RedIris:
  - BGP redirection traffic
  - Self IP Blocking
  - Mitigations tools
- Unwanted Traffic Removal Service (UTRS)
- Protección DDoS Comercial



Conclusiones

- Todo irá mal en un DDoS.
- No estamos preparados.
- Un DDoS efectivo te deja sin posibilidad de reacción.
- Poca frecuencia pero alto impacto
- No son ataques persistentes.
- Necesitas ayuda externa para su detección y mitigación.



?